FORM PTO-1390 (REV. 11-2000)
U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER
704-X00-047US

U.S. APPLICATION NO. (If known, see 37 CFR 1.5
09/807099

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/US00/21615	AUGUST 8, 2000	

TITLE OF INVENTION
HONESTY PRESERVING NEGOTIATION AND COMPUTATION

APPLICANT(S) FOR DO/EO/US
BINYAMIN PINKAS & SIMEON NAOR

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. ☐ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☒ is attached hereto (required only if not communicated by the International Bureau).
   b. ☐ has been communicated by the International Bureau.
   c. ☒ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☐ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☐ Amendments to the claims of the International Aplication under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ An English lanugage translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment.
14. ☐ A SECOND or SUBSEQUENT preliminary amendment.
15. ☐ A substitute specification.
16. ☐ A change of power of attorney and/or address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
18. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☒ Other items or information:
    COPY OF PCT REQUEST, AMENDED PAGES, FORMAL DRAWINGS AND TRANSMITTAL LETTER; EXPRESS MAILING CERTIFICATE, POSTCARD

09/807098 U.S. APPLICATION NO. (if known, see 37 CFR 1.5) | INTERNATIONAL APPLICATION NO. PCT/US00/21615 | ATTORNEY'S DOCKET NUMBER 704-X00-047US

21. ☒ The following fees are submitted: **BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):**	CALCULATIONS	PTO USE ONLY
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1000.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO **$860.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$710.00**		
International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$690.00**		
International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) **$100.00**		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 710	
Surcharge of **$130.00** for furnishing the oath or declaration later than □ 20 □ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	$	
Total claims	22 - 20 =	2	x **$18.00**	$ 36	
Independent claims	- 3 =		x **$80.00**	$	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$270.00**	$	

TOTAL OF ABOVE CALCULATIONS =	$ 746	
☒ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2. +	$ 373	
SUBTOTAL =	$ 373	
Processing fee of **$130.00** for furnishing the English translation later than □ 20 □ 30 months from the earliest claimed priority date (37 CFR 1.492(f)).	$	
TOTAL NATIONAL FEE =	$ 373	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +	$ 40	
TOTAL FEES ENCLOSED =	$ 413	
	Amount to be refunded:	$
	charged:	$

a. □ A check in the amount of $ ______________ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. 50-0601 in the amount of $ 413 to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 50-0601 A duplicate copy of this sheet is enclosed.

d. □ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

MARTIN FLEIT
FLEIT KAIN GIBBONS GUTMAN & BONGINI
520 BRICKELL KEY DR. #A201
MIAMI, FL 33131

Martin Fleit
SIGNATURE

MARTIN FLEIT
NAME

16,900
REGISTRATION NUMBER

PATENT - Attorney Docket No.: 704-X00-047US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln of: BINYAMIN PINKAS ET AL

Appln. No/Patent No.: National Stage filing based on PCT/USOO/21615

Filed/Issued: April 8, 2001

For: HONESTY PRESERVING NEGOTIATION AND COMPUTATION

CERTIFICATE OF EXPRESS MAILING

PATENTS
EXPRESS "Express Mail" Mailing Label number EF035667435US
Date of Deposit April 9, 2001

I hereby certify that this paper(s) and/or fee(s) is being deposited with the United States Postal Services "Express Mail Post Office to Addressee" service under 37 CFR §1.10 on the date indicated above and is addressed to the Commissioner of Patents & Trademark, Washington D.C. 20231.

Martin Fleit
(Signature of person mailing paper or fee)

MARTIN FLEIT
(Typed or printed name of person mailing paper or fee)

TRANSMITTAL LETTER TO THE UNITED STATES RECEIVING OFFICE

Date	09/11/00
International Application	PCT/US00/21615
Attorney Docket No.	704-X00-047PCT

I. Certification under 37 CFR 1.10 (if applicable)

EK053044745EK	09/11/00
Express Mail mailing number	Date of Deposit

I hereby certify that the application/correspondence attached hereto is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to Assistant Commissioner for Patents, Washington, D.C. 20231.

	MARTIN FLEIT
Signature of person mailing correspondence	Typed or printed name of person mailing correspondence

II. □ New International Application

TITLE		Earliest priority date (Day/Month/Year)

SCREENING DISCLOSURE INFORMATION: In order to assist in screening the accompanying international application for purposes of determining whether a license for foreign tranmittal should and could be granted and for other purposes, the following information is supplied. (Note: check as many boxes as apply):

A. □ The invention disclosed was not made in the United States.

B. □ There is no prior U.S. application relating to this invention.

C. □ The following prior U.S. application(s) contain subject matter which is related to the invention disclosed in the attached international application. (*NOTE: priority to these applications may or may not be claimed on form PCT/RO/101 (Request) and this listing does not constitute a claim for priority.*)

application no.		filed on	
application no.		filed on	

D. □ The present international application contains additional subject matter not found in the prior U.S. application(s) identified in paragraph C. above. The additional subject matter is found on pages ______ and □ **DOES NOT ALTER** □ **MIGHT BE CONSIDERED TO ALTER** the general nature of the invention in a manner which would require the U.S. application to have been made available for inspection by the appropriate defense agencies under 35 U.S.C. 181 and 37 CFR 5.1. See 37 CFR 5.15

III. ☑ A Response to an Invitation from the RO/US. The following document(s) is(are) enclosed:

A. □ A Request for An Extension of Time to File a Response

B. ☑ A Power of Attorney (General or Regular)

C. ☑ Replacement pages:

pages		of the request (PCT/RO/101)	pages	1-6	of the figures
pages	4 AND 13	of the description	pages		of the abstract
pages		of the claims			

D. □ Submission of Priority Documents

Priority document		Priority document	

E. □ Fees as specified on attached Fee Calculation sheet form PCT/RO/101 annex

IV. □ A Request for Rectification under PCT 91 □ A Petition □ A Sequence Listing Diskette

V. ☑ Other (please specify):

The person signing this form is the:		
	□ Applicant	MARTIN FLEIT REG. NO. 16,900
	☑ Attorney/Agent (Reg. No.)	Typed name of signer
	□ Common Representative	Signature

PATENT - Attorney Docket No.: 704-X00-047PCT

UNITED STATES RECEIVING OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln of: YEDA RESEARCH AND DEVELOPMENT CO. LTD.
Appln. No/Patent No.: PCT/USOO/21615
Filed/Issued: AUGUST 8, 2000
For: HONESTY PRESERVING NEGOTIATION AND COMPUTATION

LETTER

Submitted herewith together with a Transmittal Letter are corrected pages 4 and 13 of the specification which have been corrected pursuant to the Invitation to Correct Defects that was mailed 23 August 2000. The correction to these pages was necessitated by the correction to the drawings to comply with Annexes B1 and C1, attached to Invitation to Correct Defects. In the correction to the drawings, new formal drawings complying with the rules are submitted, and Figure 4, which appeared on two pages, has been corrected to Figures 4A and 4B. Accordingly, page 4 of the specification has been corrected, in the description of the Figures in line 19, to state that Figure 4 is now Figures 4A and 4B. On page 13 of the specification, line 2, the reference to Figure 4 has been changed to Figures 4A and 4B. Powers of Attorney, duly signed by all applicants are submitted herewith to cure the defect stated in Annex A. It is respectfully submitted that all defects noted have been cured, and that the application complies with the rules and regulations.

Respectfully submitted,

Martin Fleit, Attorney for Applicants, Reg. #16,900 by all other parties. This party observes the operation of the center, i.e. it examines the inputs that the center receives, verifies that the center computes the correct output, and testifies that this is the case. The invention provides the same security as is provided with this trusted party, but without using any such party. This ensures better security (since trusted parties might breach the trust they are given), and is more efficient (since it does not require an additional party).

Other and further advantages and objects of the present invention will become readily apparent when considering the following detailed description of the present invention when taken together with the appended drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram illustrating the different entities engaged in a computerized auction.

Figure 2 is a schematic diagram illustrating the steps of the method of the present invention where the steps are indicated by numerals in parentheses.

Figure 3 is a high level descriptive flow chart of the present invention as generally depicted in the diagrams of Figures 1 and 2.

Figures 4A and 4B are a flow chart showing the steps of the implementation of the preferred embodiment of the present invention.

Figure 5 is a flow chart of a secure two-party function evaluation protocol as implemented by the present invention.

Figure 6 is a schematic diagram of a gate used in the protocol depicted in Figure 5, and also shows the pseudo-random function used to prepare Table T_g used in the protocol of depicted in Figure 5.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

As initially noted, the apparatus and method of the present invention comprises an auction service that is used in a network, such as, the Internet, and uses clients and/or servers. The invention utilizes cryptography and secure distributed computation via computers to effect a computerized auction. However, the invention is not limited to computerized auctions, but has broader application.

Now the details of the implementation of the preferred embodiment will be described in conjunction with the flow chart of Figures 4A and 4B. The first stage is the announcement. This stage is carried out by the center **421** announcing in step **401** that it will compute F. Let K be a security parameter. The center constructs in step **402** K garbled circuits that compute F. For each input wire j of each of the circuits the center chooses in step **403** a random permutation P.sub.j over the two values 0 and 1. The center publishes in step **404** the tables of the gates of the K circuits **422**. For each input wire j (in each of the circuits) it publishes in step **404** a commitment to W.sub.j.sup.0 and a commitment to W.sub.j.sup.1, ordered by the permutation P.sub.j, and a commitment to P.sub.j.

The next stage is for the parties 420 to commit to their inputs. Each party B.sub.i has an input x.sub.i of l bits. The bits of this input are denoted as x.sub.(i,l). Each input bit should be input to an input wire in each of the K circuits. For each wire j of these wires, the center sends in step **405** to B.sub.i, the permutation P.sub.j. B.sub.i sends in response in step **406** a commitment **424** to P.sub.j(x.sub.(i,l)), i.e. to the permuted value of its input.

The next stage is to publish the commitments. The center **421** publishes in step **407** the commitments **424** it received from the parties.

The next stage is to open the commitments. The parties **420** choose K/2 of the K circuits that the center has created and ask the center to open in step **408** all the commitments to the permutations and garbled inputs of these K/2 circuits **423**. They verify in step **409** that these circuits indeed compute F. Each of the parties B.sub.i sends in step **410** its input x.sub.i to the center. B.sub.i also opens to the center the commitments that it made to each of its assigned input wires. These were for values 0 or 1 which are the permuted values of B.sub.i's inputs. The center verifies in step **411** that these commitments are consistent. The center publishes in step **412** the opened commitments **425** of each of the parties, and opens the garbled values W.sub.j.sup.0 or W.sub.j.sup.1 that correspond to them.

In the next stage, the center computes the function in step **413** and publishes the output of each of the K/2 circuits which were not chosen by the